IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): An apparatus for generating pseudorandom sequences comprising:

a cellular automata random number generator of a first type configured to generate a first sequence with a first predetermined randomness and a first predetermined period;

a cellular automata random number generator of a second type configured to generate a second sequence with a second predetermined randomness lower than the first predetermined randomness, and a second predetermined period larger ~~that~~ than the first predetermined period; and

adders configured to perform bit-to-bit mod2 sum of the first sequences and the second sequences.

Claim 2 (Previously Presented): The apparatus according to claim 1, wherein:

the cellular automata random number generator of a first type is two-dimensional cellular automata;

the cellular automata random number generator of a second type is 2-by-L cellular automata; and

summation results from the adders are outputted as the pseudorandom sequences.

Claim 3 (Previously Presented): The apparatus according to claim 1, further comprising:

a cellular automata random number generator of a third type configured to generate a third sequence, the cellular automata random number generator of a third type determines cell

states based on a corresponding cell control word and/or a corresponding rule control word;

wherein

the cell control word is generated by the cellular automata random number generator of a second type;

the rule control word is generated by the cellular automata random number generator of a first type; and

the adders perform bit-to-bit mod2 sum of the first, the second and the third sequences.

Claim 4 (Previously Presented): The apparatus according to claim 3, wherein:

the summation results from the adders are outputted as pseudorandom sequences.

Claim 5 (Previously Presented): The apparatus according to claim 2 further comprising:

a first block configured to perform a nonlinear mapping on the summation results from the adders; and

a second block configured to perform a non-uniform decimation on the results of the nonlinear mapping, wherein the decimated result is outputted as the pseudorandom sequence.

Claim 6 (Previously Presented): The apparatus according to claim 5, wherein:

each of the blocks includes at least one nonlinear function.

Claim 7 (Previously Presented): The apparatus according to claim 5, wherein:

the second block includes at least one look-up table for nonlinear mapping based on the Latin squares.

Claim 8 (Previously Presented): An apparatus for performing cryptographic processing comprising:

a cryptographic processor for encrypting data using pseudorandom sequences; and

a pseudorandom sequence generator for generating pseudorandom sequences, wherein the pseudorandom number generator is configured to include the apparatus according to claim 1.

Claim 9 (Currently Amended): A method for generating pseudorandom sequences using cellular automata in a pseudorandom sequence generator comprising:

generating, at a cellular automata random number generator of a first type, a first sequence with a first predetermined randomness and a first predetermined period;

generating, at a cellular automata random number generator of a second type, a second sequence with a second predetermined randomness lower than the first predetermined randomness, and a second predetermined period larger ~~that~~ than the first predetermined period; and

performing, at an adder, bit-to-bit mod2 sum of the first sequences and the second sequences.

Claim 10 (Canceled).

Claim 11 (Currently Amended): A non-transitory computer readable recording medium storing a computer program for causing a computer to execute a method for generating pseudorandom sequences using cellular automata, the ~~the~~ method comprising:

generating a first sequence with a first predetermined randomness and a first predetermined period;

generating a second sequence with a second predetermined randomness lower than the first predetermined randomness, and a second predetermined period larger ~~that~~ than the first predetermined period; and

performing bit-to-bit mod2 sum of the first sequences and the second sequences.

Claim 12 (Previously Presented): The apparatus according to claim 1, wherein the first sequence generated by the cellular automata random number generator of a first type satisfies the DIEHARD test.

Claim 13 (New): The apparatus according to claim 2, wherein the cellular automata random number generator of a first type generates two-dimensional cellular automata including 64 cells.

Claim 14 (New): The apparatus according to claim 2, wherein the cellular automata random number generator of a first type generates two-dimensional cellular automata arranged in an 8x8 array.

Claim 15 (New): The apparatus according to claim 1, further comprising:

a buffer configured to buffer results of the bit-to-bit mod2 sum.

Claim 16 (New): The apparatus according to claim 2, wherein the adders output pseudorandom sequences with a controllable period.

Claim 17 (New): The apparatus according to claim 3, wherein the cellular automata random number generator of the third type includes a plurality of cell units.

Claim 18 (New): The method for generating pseudorandom sequences according to claim 9, further comprising generating a key for cryptographic processing based on the generated pseudorandom sequences.

Claim 19 (New): The method for generating pseudorandom sequences according to claim 9, further comprising interfacing with an external device.

Claim 20 (New): The method for generating pseudorandom sequences according to claim 19, wherein the interfacing includes inputting information designating the key to be used and outputting encrypted text data based on the key.